(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) Offenlegungsschrift

(10) DE 101 02 779 A 1

(51) Int. Cl.[7]: H 04 L 9/32

(21) Aktenzeichen: 101 02 779.6
(22) Anmeldetag: 22. 1. 2001
(43) Offenlegungstag: 29. 8. 2002

DE 101 02 779 A 1

(71) Anmelder:
Utimaco Safeware AG, 61440 Oberursel, DE

(74) Vertreter:
Wagner, M., Dipl.-Ing., Pat.-Anw., 52068 Aachen

(72) Erfinder:
Gohmann, Stefan, 52062 Aachen, DE; Micus, Frank, 52062 Aachen, DE; Philipp, Andreas, 52070 Aachen, DE; Vennemann, Ralf, 52062 Aachen, DE

(56) Entgegenhaltungen:

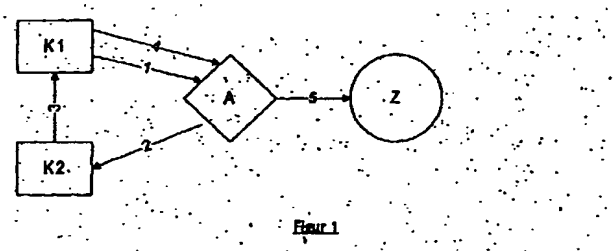
DE	197 22 424 C1
DE	197 18 103 A1
WO	95 19 593 A1
WO	00 45 247 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

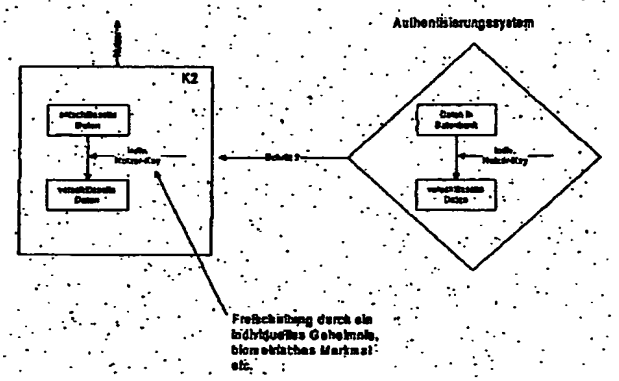
Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Autorisierung in Datenübertragungssystemen

(57) Es ist ein Verfahren zur Autorisierung in Datenübertragungssystemen, bei dem ein Nutzer über zwei getrennte erste und zweite Datenkommunikationseinrichtungen K1, K2 über ein Authentisierungssystem A Zugang zu einem System Z gelangen möchte, offenbart, mit dem die Sicherheit gegenüber herkömmlichen Systemen durch Verwendung einer kryptographischen Verschlüsselung zwischen dem Authensisierungssystem A und der Datenkommunikationseinrichtung K2 erhöht wird.



Figur 1



DE 101 02 779 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Autorisierung in Datenübertragungssystemen. Bei einem solchen Verfahren möchte, wie die Fig. 1 zeigt, ein Nutzer über zwei getrennte erste und zweite Datenkommunikationseinrichtungen K1, K2 über ein Authentisierungssystem A Zugang zu einem System Z erlangen.

[0002] Ein bekanntes derartiges Verfahren (vgl. z. B. DE 197 18 103 A1) sieht hierzu vor,

- daß der Nutzer in einem 1. Schritt über die erste Datenkommunikationseinrichtung K1 unter Angabe von ihn eindeutig in einer Nutzerdatenbank lokalisierenden Informationen wie UserID od. dgl. eine Anfrage an ein Authentisierungssystem A stellt;
- daß in einem 2. Schritt das Authentisierungssystem A für den Nutzer eine Transaktionsnummer TAN oder ein vergleichbares Passwort generiert oder aus einer Datei auswählt;
- daß in einem 3. Schritt das Authentisierungssystem A die TAN oder das vergleichbare Passwort an eine zweite Datenkommunikationseinrichtung K2 übermittelt;
- daß in einem 4. Schritt die TAN oder das vergleichbare Passwort von der zweiten Datenkommunikationseinrichtung K2 an die erste Datenkommunikationseinrichtung K1 übermittelt wird;
- daß in einem 5. Schritt die TAN oder das vergleichbare Passwort von der ersten Datenkommunikationseinrichtung K1 an das Authentisierungssystem A übermittelt wird;
- daß in einem 6. Schritt das Authentisierungssystem A die Gültigkeit der TAN oder des vergleichbaren Passworts prüft, um dann
- in einem 7. Schritt einen Verbindungsaufbau zwischen der Datenkommunikationseinrichtung K1 und dem System Z herzustellen oder freizuschalten.

[0003] Dieses Verfahren beinhaltet jedoch einen schwerwiegenden Nachteil bzw. eine Sicherheitslücke:
Im Stand der Technik ist nämlich die Übermittlung der TAN oder des vergleichbaren Passworts lediglich durch die systembedingte Geräteeigenschaft der Datenkommunikationseinrichtung K2 abgesichert. Dies bedeutet, daß zwar die TAN oder das vergleichbare Passwort während der Übertragung z. B. gegen Abhören (mehr oder weniger) abgesichert ist, daß jedoch am Ende der Übertragung die TAN oder das vergleichbare Passwort in jedem Falle auf der Datenkommunikationseinrichtung im Klartext dargestellt wird. Es wird dabei im Stand der Technik also davon ausgegangen, daß lediglich der berechtigte Nutzer Zugang zur Datenkommunikationseinrichtung K2 hat. Ist jedoch durch Unachtsamkeit oder Diebstahl ein anderer Nutzer im Besitz der Datenkommunikationseinrichtung K2, bringt das vorgeschlagene Verfahren des Versandes der TAN über getrennte Kommunikationskanäle keinen zusätzlichen sicherheitsrelevanten Vorteil.

[0004] Bezogen auf eine übliche Hardwarerealisierung hieße dies: Befindet sich ein Angreifer am Arbeitsplatz (Datenkommunikationseinrichtung K1) des berechtigten Nutzers und ist der Angreifer auch im Besitz des Mobiltelefons (Datenkommunikationseinrichtung K2) des berechtigten Nutzers, weil dieser es z. B. auf seinem Schreibtisch hat liegen lassen, kann der Angreifer erfolgreich auf das System Z (Bankrechner) zugreifen. Die TAN oder das vergleichbare Passwort wird zwar während der Übertragung durch die vorhandene Verschlüsselung im Mobilfunknetz (z. B. GSM-Standard) gesichert. Allerdings kann bei entsprechender Sachkenntnis die TAN oder das vergleichbare Passwort bei der Übertragung abgefangen und verwendet werden. Selbst wenn Sie nicht abgefangen oder so aufwendig verschlüsselt wird, daß ein Abfangen praktisch unmöglich wird, erscheint sie am Ende der Übertragung im Display des Mobiltelefons als Klartext und steht damit dem Angreifer in der oben beschriebenen Situation zur Verfügung.

[0005] Es ist daher Aufgabe der vorliegenden Erfindung, unter Vermeidung der aus dem Stand der Technik bekannten Nachteile ein Verfahren zur Autorisierung in Datenübertragungssystemen anzugeben, in dem die Sicherheit erhöht wird.

[0006] Diese Aufgabe wird bei einem gattungsgemäßen Verfahren gelöst, das die kennzeichnenden Merkmale des Patentanspruchs 1 aufweist.

[0007] Dadurch, daß die Übermittlung zwischen dem Authentisierungssystem A und der Datenkommunikationseinrichtung K2 mittels eines kryptographischen Verfahrens verschlüsselt wird, ergibt sich in Fortbildung des Standes der Technik eine sichere und eindeutige Authentikation des Nutzers.

[0008] Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

[0009] Die Erfindung wird nachstehend anhand bevorzugter Ausführungsformen näher erläutert, wobei die Komponenten kurz wie folgt charakterisiert werden:
Unter Datenkommunikationseinrichtungen K1, K2 werden solche verstanden, die Daten empfangen, in die Daten eingegeben, eingespielt und/oder an die Daten gesendet werden können. Dabei muß K2 mit einer Zusatzapplikation ausgestattet sein bzw. muß diese nachladbar sein (auch z. B. durch Austausch von SIM-Karten), die die Verschlüsselungsverfahren nutzen kann. Wie weiter unten beschrieben wird, können bei Anwendung des erfindungsgemäßen Verfahrens die Datenkommunikationseinrichtungen K1, K2 ohne Sicherheitsverlust sogar innerhalb eines Gerätes realisiert werden.

[0010] Der Nutzer, der sowohl Zugriff auf K1 und K2 hat, möchte über K1 Zugang zu Z erlangen, beispielsweise ist K1 ein öffentlich zugänglicher Rechner, über den eine Preisliste eines E-Shops auf Z eingesehen werden soll. K2 stellt dann das Hilfsmittel dar, um sich gegenüber Z sicher zu authentisieren. K2 kann z. B. ein Mobiltelefon oder ein Personal Digital Assistent (PDA) sein.

[0011] Bei dem Authentisierungssystem A handelt es sich um ein Rechnersystem mit einer internen oder auch ausgelagerten geschützten Datenbank mit teilweise verschlüsselten Nutzerinformationen (Name, UserID, Identifikationsmerkmal von K2 (z. B. Mobilnummer) und individueller Schlüssel zur Kommunikation mit K2 etc.), mit einer sicheren Generierungseinheit für Passwörter (Zugangscodes, zeitlich begrenzt gültige Passwörter) und mit einem implementierten Verfahren zur individuellen Verschlüsselung von Nutzerinformationen und/oder (auch zeitlich begrenzter) Passwörter für den Nutzer. Es versteht sich, daß das Rechnersystem aus mehreren Einzelsystemen bestehen kann.

[0012] Die Zugangseinheit bzw. das System Z ist die Einheit, zu der der Benutzer Zugang oder von der der Benutzer Daten haben möchte, beispielsweise eine Datenkommunikationseinrichtung, eine Zutrittsvorrichtung (Türen, Schließfächer, Parkplätze etc.) oder ein Zahlungssystem.

[0013] Nachstehend wird ein bevorzugter Verfahrensablauf beschrieben:
Der Nutzer stellt über die Datenkommunikationseinrichtung K1 eine Anfrage an das Authentisierungssystem A. Übermittelt werden u. a. Informationen (z. B. UserID), die den Nutzer eindeutig in der Nutzerdatenbank oder einem ande-

ren geeigneten Speichermedium lokalisieren. Diese notwendigen Daten des Benutzers wie selbstgewählte UserID, Name, Mobilfunknummer etc. wurde zuvor in einem einmaligen Anmeldeprozeß in der Benutzerdatenbank eingetragen.

[0014] Kann bei der Anfrage der Eintrag in der Datenbank lokalisiert werden, wird ein Passwort, vorzugsweise ein Einmalpasswort (OTP One Time Pin), generiert und mit dem individuellen Schlüssel des Nutzers aus der Datenbank verschlüsselt an K2 übermittelt. Das Authentisierungssystem speichert das Passwort in der kryptographisch gesicherten Datenbank im Nutzerdatensatz, evtl. mit einer Gültigkeitsangabe. Der Vorteil der kryptographisch gesicherten Datenbank besteht darin, daß lediglich die UserID im Klartext lesbar ist, alle weiteren Daten hingegen verschlüsselt und somit für Angreifer wertlos sind.

[0015] Zur gesicherten Übermittlung des Einmalpasswortes an den Benutzer wird der Public-Key-Algorithmus verwendet. Alle verwendeten Schlüssel auf der Seite des Authentisierungsdienstes sind in einem Hardware-Sicherheitsmodul gesichert abgelegt und somit gegen unberechtigten Zugriff geschützt.

[0016] Das Einmalpasswort ist während der Übertragung zum Mobiltelefon über ein asymmetrisches Verfahren verschlüsselt.

[0017] Von K2 kann das Passwort automatisch oder – wie in der Fig. 2 dargestellt – auf Anwendungsebene vom Nutzer durch die zusätzliche Eingabe eines Identifizierungsmerkmales entschlüsselt werden. Dies kann z. B. bei einer SIM-Karte der neuen Generation über die auf dieser abgelegten, PIN-geschützten Zusatzapplikation erfolgen.

[0018] Ist dies erfolgreich, werden die Daten der Kommunikationseinrichtung K2 angezeigt, so daß der Nutzer das Passwort entnehmen und über K1 dem Authentisierungssystem A zur Prüfung vorlegen kann. Es ist jedoch auch möglich, die Daten unmittelbar weiterzuverarbeiten. In beiden Fällen erhält der Nutzer bei erfolgreicher Authentisierung Zugriff auf Z.

[0019] Zur Verschlüsselung können neben Public-Key-Verfahren auch Verfahren mit vergleichbaren Eigenschaften zum Einsatz kommen. Der Schlüssel muss wie dargestellt dem Nutzer eindeutig zugeordnet sowie auf einem sicheren Medium im Besitz des Nutzers gespeichert sein. Dies kann die SIM-Karte des Mobiltelefons, aber auch andere Smartcards oder ein wiederbeschreibbaren Speichermedium sein. Die Freischaltung des Schlüssels muß an ein Geheimnis gebunden sein, welches nur dem Nutzer zugeordnet und nicht bereits durch den Zugriff auf K2 erhältlich ist, beispielsweise eine PIN, ein biometrisches Verfahren od. dgl.

[0020] Das beschriebene Verfahren kann aufgrund der weiten Verbreitung mobiler Telefone oder auch PDAs als Endgeräte des zweiten Übertragungskanals bereits heute einem großen Benutzerkreis zur Verfügung gestellt werden.

Patentansprüche

1. Verfahren zur Autorisierung in Datenübertragungssystemen, bei dem ein Nutzer über eine erste Datenkommunikationseinrichtung (K1) Zugang zu einem System (Z) erlangen möchte, wobei
der Nutzer in einem 1. Schritt über die erste Datenkommunikationseinrichtung (K1) unter Angabe von ihn eindeutig in einer Nutzerdatenbank lokalisierenden Informationen wie UserID od. dgl. eine Anfrage an ein Authentisierungssystem (A) stellt;
in einem 2. Schritt das Authentisierungssystem (A) für den Nutzer eine Transaktionsnummer (TAN) oder ein vergleichbares Passwort generiert oder aus einer Datei auswählt;
in einem 3. Schritt das Authentisierungssystem (A) die TAN oder das vergleichbare Passwort an eine zweite Datenkommunikationseinrichtung (K2) übermittelt;
in einem 4. Schritt die TAN oder das vergleichbare Passwort von der zweiten Datenkommunikationseinrichtung (K2) an die erste Datenkommunikationseinrichtung (K1) übermittelt wird;
in einem 5. Schritt die TAN oder das vergleichbare Passwort von der ersten Datenkommunikationseinrichtung (K1) an das Authentisierungssystem (A) übermittelt wird;
in einem 6. Schritt das Authentisierungssystem (A) die Gültigkeit der TAN oder des vergleichbaren Passworts prüft, um dann
in einem 7. Schritt einen Verbindungsaufbau zwischen der Datenkommunikationseinrichtung (K1) und dem System (Z) herzustellen oder freizuschalten,
dadurch gekennzeichnet, daß
die Übermittlung zwischen dem Authentisierungssystem (A) und der Datenkommunikationseinrichtung (K2) mittels eines kryptographischen Verfahrens verschlüsselt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß als kryptographisches Verschlüsselungsverfahren ein symmetrisches Verfahren eingesetzt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß als kryptographisches Verschlüsselungsverfahren ein asymmetrisches Verfahren eingesetzt wird.

4. Verfahren nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der zur Entschlüsselung der übertragenen TAN oder des vergleichbaren Passworts erforderliche Schlüssel von dem Benutzer in die Datenkommunikationseinrichtung (K2) eingegeben wird.

5. Verfahren nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der zur Entschlüsselung der übertragenen TAN oder des vergleichbaren Passworts erforderliche Schlüssel in der Datenkommunikationseinrichtung (K2) abgelegt und durch Eingabe eines individuellen Geheimnisses des Nutzers freigeschaltet wird.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß das individuelle Geheimnis eine PIN od. dgl. ist.

7. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß das individuelle Geheimnis durch ein biometrisches Verfahren gewonnen wird.

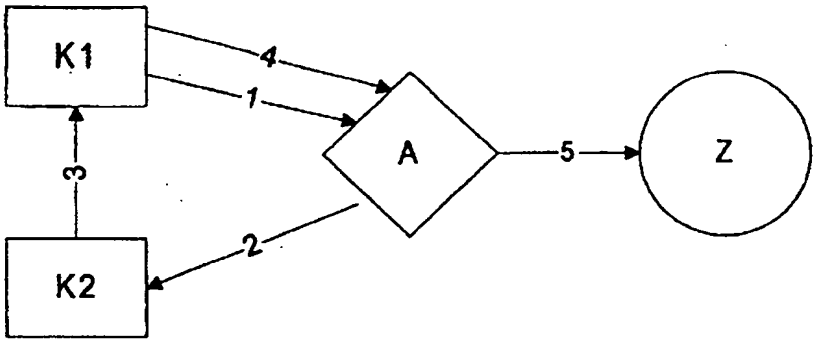
8. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Nutzer die an das Authentisierungssystem (A) zur Generierung eines Passworts gerichtete Anfrage statt über die erste Datenkommunikationseinrichtung (K1) über die Datenkommunikationseinrichtung (K2) stellt;

9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, daß die Anfrage mittels eines kryptographischen Verfahrens verschlüsselt wird.

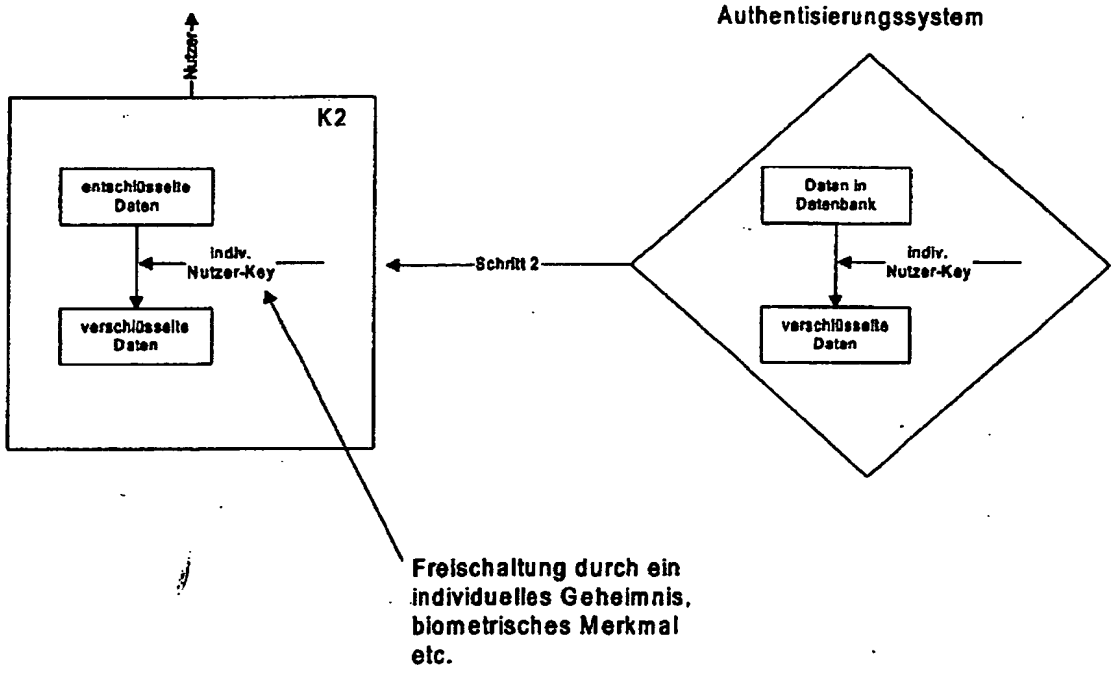
10. Vorrichtung zur Durchführung des Verfahrens nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Datenkommunikationseinrichtungen (K1, K2) in einem Gerät zusammengefaßt sind.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 101 02 779 A1
Int. Cl.[7]: H04L 9/32
Offenlegungstag: 29. August 2002



Figur 1



Figur 2